

RDC SmartPay Business User Maintenance

# **QUICK REFERENCE GUIDE**

## SmartPay Business User Maintenance

Admin users are responsible for creating user profiles for those completing tasks with the SmartPay Business application on a daily basis. The admin user is also responsible for updating user profiles, providing new passwords, unlocking users in the event they become locked out of the system, and deleting a user's profile if necessary.

1. Log in to SmartPay Business, and then select **Admin | Users** from the left main menu.

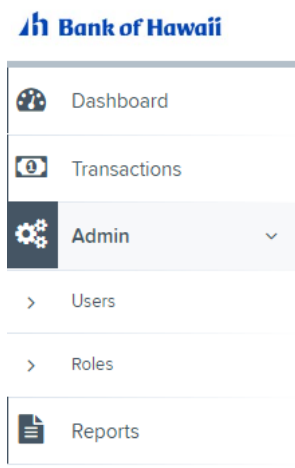
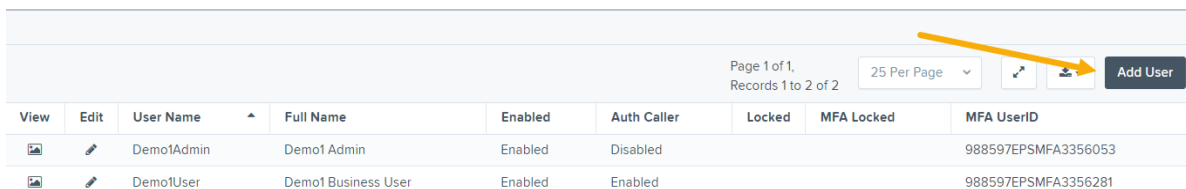


Figure 1

2. Select **Add User**.



View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		Demo1Admin	Demo1 Admin	Enabled	Disabled			988597EPSMFA3356053
		Demo1User	Demo1 Business User	Enabled	Enabled			988597EPSMFA3356281

Figure 2

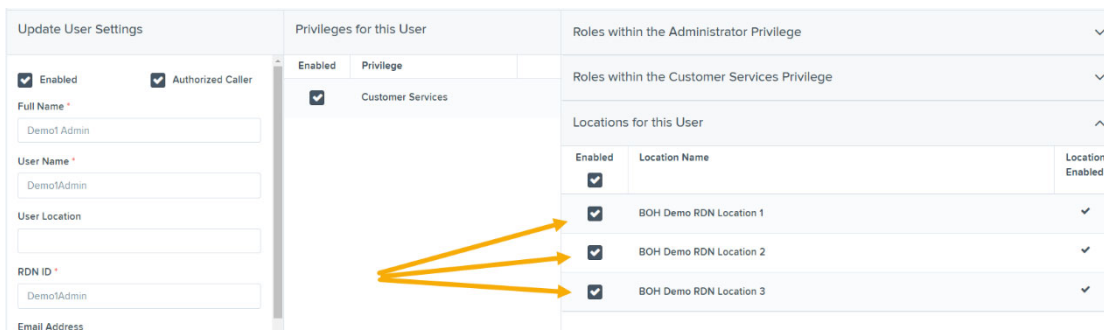
3. Fill in the following required fields.

- **Full Name** – The first and last name of the user.
- **User Name** – The user's login name. This field is not case-sensitive.
- **RDN ID** – This field will create the RDN user on the backend. It can be the same as the profile user name. To avoid duplication of the user profiles, do not update this field after the original setup.

Non-required fields:

- **Email Address** – The email address of the user.
- **User Location** – Optional informational field to describe the user.
- **Auto Disable** – This field is not used currently.

- **Dual Auth Amount** – This field is not used currently.
  - **Dual Auth Status** – This field is not used currently.
4. Fill out the additional *Add User Settings* and the *Privileges for this User* sections. Note that a **Temporary Password** is displayed at the bottom of the page—provide this password to the user you are creating.
    - a. Select the **Authorized Caller** check box if this user will contact EPS for support, if necessary. Once enabled, the user will then be required to establish an **Authorized Caller Identification Phrase** that will be used by the EPS Customer Support representative to verify that the user is authorized before providing support. Callers who are not able to answer their identification phrase, or are not an authorized user will be directed to their financial institution for further assistance.
    - b. Once you have selected privileges to provide to this user, select **Add**. The system will create the user and allow you to select roles underneath each of the privileges assigned to them.
  5. Under *Roles within the Customer Service* privilege, select the *Accounting* role for the user to run reports in the application. Select the *Remote Deposit Now* role for the user to scan checks to submit for deposit using RDN. Select mRDC role for the user to be able to use the mobile app to scan checks to submit for deposit through RDN.
  6. Select the appropriate check boxes under *Locations for this User* for which the user will scan checks.



Update User Settings		Privileges for this User		Roles within the Administrator Privilege		
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Authorized Caller	Enabled	Privilege	Roles within the Customer Services Privilege		
Full Name *		<input checked="" type="checkbox"/>	Customer Services	Locations for this User		
Demo1 Admin				Enabled	Location Name	Location Enabled
User Name *				<input checked="" type="checkbox"/>	BOH Demo RDN Location 1	<input checked="" type="checkbox"/>
Demo1Admin				<input checked="" type="checkbox"/>	BOH Demo RDN Location 2	<input checked="" type="checkbox"/>
User Location				<input checked="" type="checkbox"/>	BOH Demo RDN Location 3	<input checked="" type="checkbox"/>
RDN ID *						
Demo1Admin						
Email Address						

Figure 3

7. Select **Update** at the bottom of the page.

## Enabling Remote Deposit Now (RDN) Features for a User Profile

Remote Deposit Now (RDN) is the tool within SmartPay Business used to scan check deposits. To specify the permissions this user will have with RDN, select the check box next to the *Enable RDN* option on the *Update User Settings* page, and select **Update** at the bottom of the page. You may need to scroll down within the *Update User Settings* pane to view this option. The page refreshes, and the various permissions to give a user profile appear.

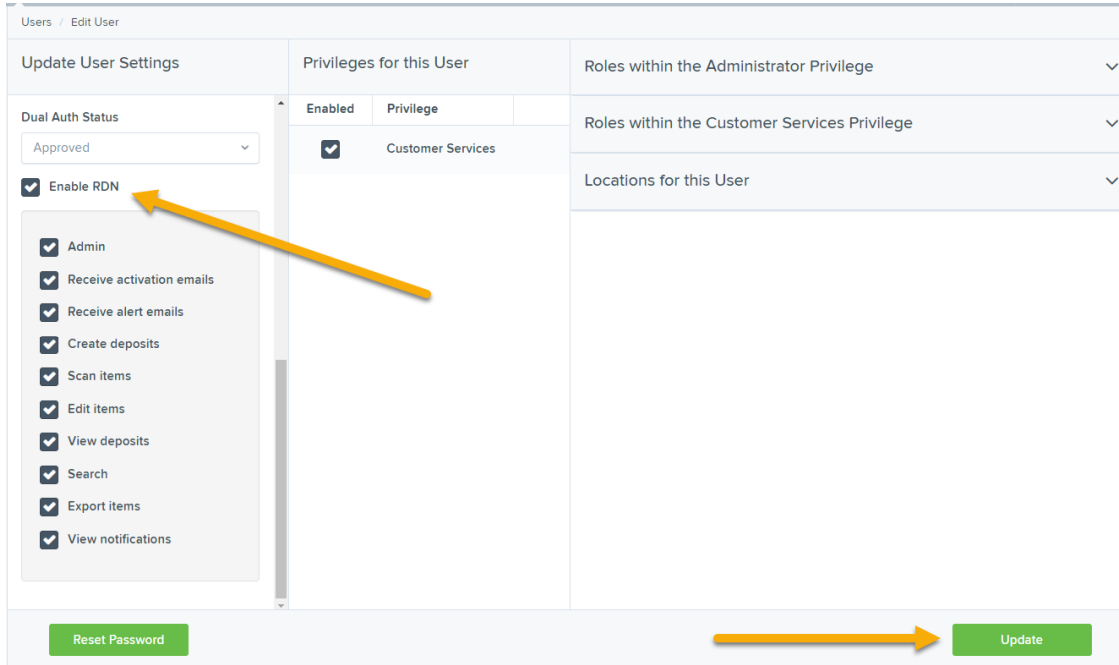
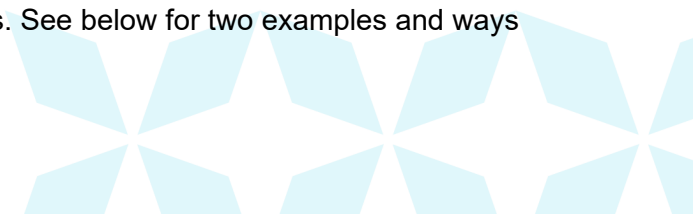


Figure 4

1. Select which RDN permissions the user will need from the options displayed.
  - **Admin Permission** – Separate from the account administrator role. This role is required to access the *Tools* tab, which allows the user to delete an existing batch.
  - **Receive Alert Emails** – Allows the user to receive deposit alert emails upon deposit.
  - **Scan Items** – Allows the user to scan items through RDN.
  - **View Deposits** – Allows the user to view deposits in RDN.
  - **Export Deposits** – Allows the user to export items.
  - **Receive Activation Emails** – Not applicable, do not check this box.
  - **Create Deposits** – Check this box to allow the user to make deposits to EPS.
  - **Edit Items** – Check this box to allow the user to be able to modify/fix their batches in RDN.
  - **Search** – This allows the user to be able to perform searches in RDN on the *Search* page.
  - **View Notifications** – This allows the user to view any deposit messages coming from EPS, such as exceeded transaction limits.
2. Make any other changes to this profile, and select **Update** at the bottom of the page to finish and save changes.

## Troubleshooting Tips

There are instances that may generate duplicate RDN alert emails. See below for two examples and ways to avoid those situations.



**Duplicated email addresses** – For every instance of the same email address that is entered into the merchant user’s profiles in SmartPay Business, the application will send an email. For example using the same email address for both the Admin profile and the merchant user will cause two identical emails to be sent to that address.

**Updating the RDN ID** – When the original RDN ID is created in the user profile, the application creates an RDN profile on the backend. If the RDN ID is changed after the initial setup, another RDN profile that is not visible to the customer will be created. This new RDN profile will contain the same information as the original profile, including the email address. This will result in multiple emails sent to the same address. To avoid this, do not make changes to the RDN ID.

## Updating a User Profile

As the admin user, you also have the responsibility of enabling/disabling users, deleting a user, resetting a user’s password, editing/updating user profiles, and designating authorized callers.

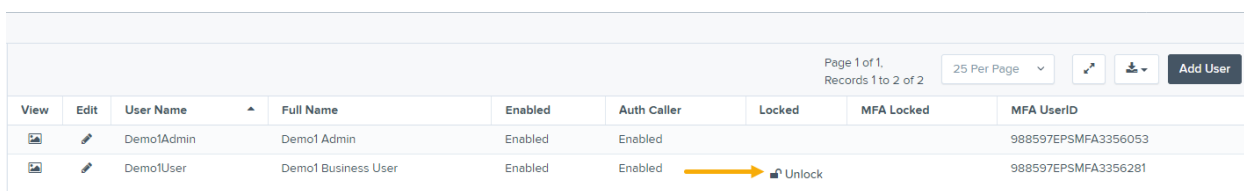
1. Log in and then select **Admin | Users** from the left main menu.
2. Select the **Edit** icon for the user profile to be updated (in this case, a user). You may also use the Filters bar to search by User Name or Full Name.
3. The *Update User Settings* page displays. Make any changes necessary to the user profile, privileges, roles, or locations for the user.
4. Click **Update** at the bottom of the page.

## Unlocking a User Profile

Users can be locked out of the system for keying their password incorrectly five times, or answering the secret question incorrectly when requesting a new temporary password.

As the admin user, you are responsible for unlocking an employee’s profile. If an admin user is locked out, contact your first line of support for assistance. Follow the steps below to unlock a user’s profile.

1. Log in and then select **Admin | Users** from the left main menu.
2. Under the *Locked* column, select the **Unlock** option for that user. The *Unlock* will disappear, and the user profile will be unlocked.



View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		Demo1Admin	Demo1 Admin	Enabled	Enabled			988597EPSMFA3356053
		Demo1User	Demo1 Business User	Enabled	Enabled			988597EPSMFA3356281

Figure 5

**NOTE:** If the user needs a new password, you will need to reset the password (detailed below).

---

## Resetting a Password

Users may forget their password and ask you to provide them with a new, temporary one. The steps below explain how to reset a user's password.

1. Log in and then select **Admin | Users** from the left main menu.
2. Select **Edit** for the user profile to update.
3. Select **Reset Password** button from the bottom of the page. The user's profile will have a case-sensitive temporary password generated. Carefully record this password and provide it to the user.

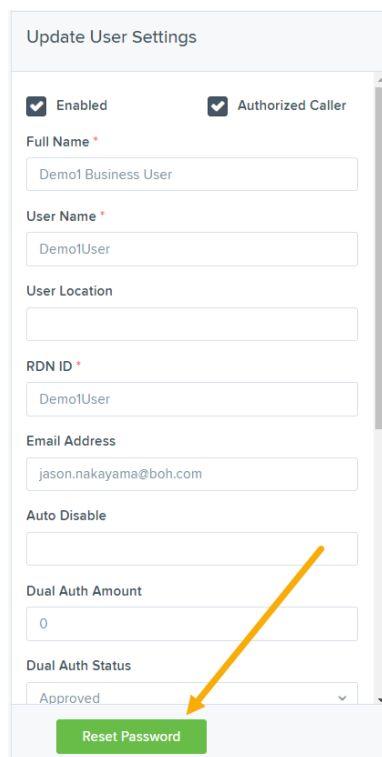
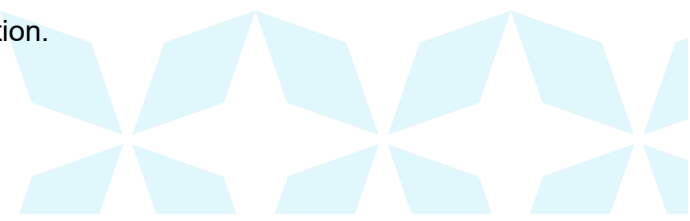


Figure 6

## Disabling a user profile

Disabling a user keeps the profile intact until access is re-enabled by the admin user. The admin may want to disable a user if a user is on leave for an extended period of time before working with the application again.

1. Log in to the system, and then select **Admin | Users** from the left main menu.
2. Select **Edit** for the user profile you wish to disable.
3. Uncheck the **Enabled** box in the *Update User Settings* section.



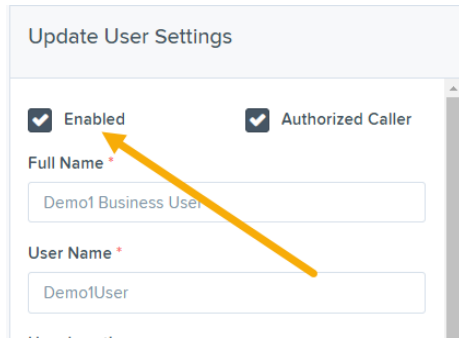


Figure 7

4. Select **Update** to save all changes.

## Deleting a User Profile

Deleting a user profile will remove it from the list of users and make it inaccessible. The *User Name* for that profile cannot be utilized again for a different user. The profile will be categorized as a deleted user. To delete an admin, you must first remove the *Administrator* privilege from the user's profile before completing the following steps.

1. Log in to the system and then select **Admin | Users** from the left main menu.
2. Select **Edit** for the user profile to delete.
3. Select **Delete User**, as shown below.

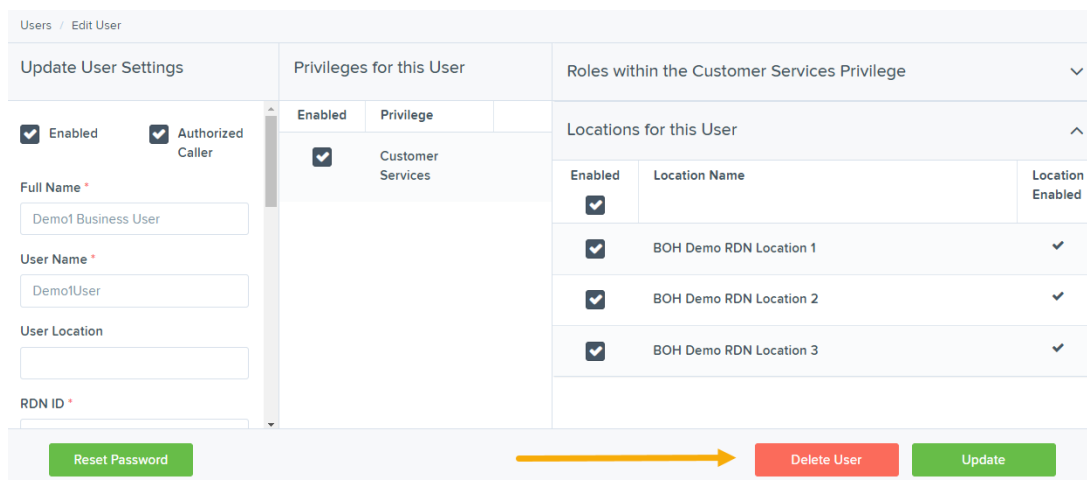


Figure 8



4. A prompt will ask you to confirm deleting the user. Select **Yes**.

Confirm Delete

Are you sure you want to delete this user?

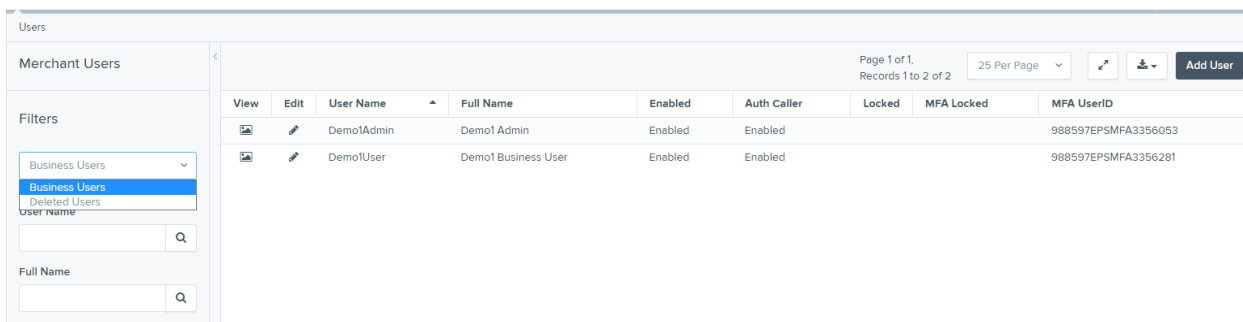
**Yes** No

Figure 9

## Listing Deleted Profiles

A list of the user profiles that you have deleted is available if you need to refer back to a previous user's profile information. This list will also provide the profile's audit history and any updates that may have been made to it.

1. Log in and then select **Admin | Users** from the left main menu.
2. In the *Merchant Users* section, select the **Deleted Users** option under *Filters*. The list of users will automatically update to display only deleted users.
  - a. Select **Clear Filters** to strip any filters from the list of users.



The screenshot shows the 'Users' management interface. On the left, there is a 'Merchant Users' section with a 'Filters' dropdown menu. The 'Filters' menu is open, showing 'Business Users' and 'Deleted Users' options. The 'Deleted Users' option is selected. Below the filters, there are search boxes for 'User Name' and 'Full Name'. The main area displays a table of users. The table has columns for 'View', 'Edit', 'User Name', 'Full Name', 'Enabled', 'Auth Caller', 'Locked', 'MFA Locked', and 'MFA UserID'. There are two rows of data. The first row is for 'Demo1Admin' and the second row is for 'Demo1User'. The 'Demo1User' row is highlighted. The table also shows 'Page 1 of 1, Records 1 to 2 of 2' and '25 Per Page'.

View	Edit	User Name	Full Name	Enabled	Auth Caller	Locked	MFA Locked	MFA UserID
		Demo1Admin	Demo1 Admin	Enabled	Enabled			988597EPSMFA3356053
		Demo1User	Demo1 Business User	Enabled	Enabled			988597EPSMFA3356281

Figure 10





